US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary
- October 2010 -

This report summarizes general activity as well as updates made to the National Cyber Alert System in October 2010. It includes current activity updates, technical and non-technical cyber security alerts, cyber security bulletins, and cyber security tips, in addition to other newsworthy events or highlights.

Executive Summary

During September 2010, US-CERT issued 18 Current Activity entries, three Technical Cyber Security Alerts, two Cyber Security Alerts, four weekly Cyber Security Bulletins, and one Cyber Security Tip.

Highlights for this month include updates or advisories released by Adobe, Foxit, Microsoft, Oracle, RIM, RealNetworks, Google, Apple, Cisco, and Mozilla; fraud advisories for businesses and consumers; and featured security tips for National Cyber Security Awareness Month.

Contents

Current Activity

Current Activity entries are high-impact security threats and vulnerabilities presently being reported to US-CERT. The table lists all of the entries posted this month followed by a brief overview of the most significant entries.

Current Activity for October 2010	
October 6	Adobe Releases Security Updates for Reader and Acrobat
October 7	Foxit Releases Foxit Reader 4.2
October 7	Microsoft Releases Advance Notification for October Security Bulletin
October 8	Oracle Releases Pre-Release Announcement for October 2010
October 12	Microsoft Releases October Security Bulletin
October 13	Oracle Releases Critical Patch for October 2010
October 14	RIM Releases Security Advisory for Blackberry Enterprise Server
October 18	RealNetworks Releases Security Update for RealPlayer Vulnerabilities
October 20	Google Releases Chrome 7.0.517.41

Current Activity for October 2010	
October 21	Apple Releases Java for Mac OS X 10.5 Update 8 and Java for Mac OS X 10.6 Update 3
October 25	Adobe Releases Security Advisory for Shockwave Player
October 25	Linux Root Access Vulnerabilities
October 25	Fraud Advisory for Businesses Released: Corporate Account Take Over
October 25	Fraud Advisory for Consumers Released: Involvement in Criminal Activity Through Work from Home Scams
October 27	Cisco Releases Security Advisory for CiscoWorks Common Services
October 27	Firefox 3.5 and 3.6 Vulnerability
October 28	Adobe Releases Security Bulletin for Flash Player, Reader, and Acrobat
October 29	Adobe Releases Security Update for Shockwave Player

- Adobe addressed multiple vulnerabilities in Acrobat, Reader, Flash Player, and Shockwave:
  - Security Advisory APSB10-21 addressed critical vulnerabilities affecting Adobe Reader and Acrobat versions 9.3.4 and earlier versions for Windows, Macintosh and UNIX, and Adobe Reader and Acrobat versions 8.2.4 and earlier for Windows and Macintosh. These updates address multiple vulnerabilities including those described in Adobe security advisory APSA10-02 and Flash Player security bulletin APSB10-22. Exploitation of this actively exploited vulnerability could cause the application to execute arbitrary code and could potentially allow an attacker to take control of the affected system.
  - Security Advisory APSA10-05 alerted users to a critical vulnerability in multiple versions of Adobe Flash Player, Reader and Acrobat. This vulnerability may allow an attacker to execute arbitrary code or cause a denial-of-service condition.
  - Security Advisories APSA10-04 and APSB10-25 alerted users of vulnerabilities affecting Adobe Shockwave Player 11.5.8.612 and earlier versions on the Windows and Macintosh operating systems. Exploitation of this vulnerability may allow an attacker to execute arbitrary code or cause a denial-of-service condition.
- Foxit released Foxit Reader 4.2 to address multiple vulnerabilities. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code, compromise the digital signature of PDF signatures or cause a denial-of-service condition.
- Microsoft released its October Security Bulletin to address vulnerabilities in Microsoft Windows, .NET Framework, Server Software, Office, and Internet Explorer. These vulnerabilities may allow an attacker to execute arbitrary code, obtain sensitive information, operate with elevated privileges, cause a denial-of-service condition, or tamper with data.
- Oracle released its Critical Patch Update for October 2010 to address 85 vulnerabilities across multiple products:
  - 7 for Oracle Database Server
  - 8 for Oracle Fusion Middleware
  - 1 for Oracle Enterprise Manager Grid Control
  - 6 for Oracle E-Business Suite
  - 2 for Oracle Supply Chain Products Suite
  - 21 for Oracle PeopleSoft and JDEdwards Suite
  - 4 for Oracle Siebel Suite
  - 1 for Oracle Primavera Products Suite

  - 26 for Oracle Sun Products Suite
  - 5 for Oracle Open Office Suite
  - 4 for Oracle VM

- RIM released security advisory KB24547 to address a vulnerability in the PDF distiller of the BlackBerry attachment service for the BlackBerry Enterprise Server. This vulnerability may allow an attacker to execute arbitrary code or cause a denial-of-service condition.
- RealNetworks addressed multiple vulnerabilities affecting RealPlayer in its security advisory. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code.
- Google released Chrome 7.0.517.41 for Linux, Mac, and Windows to address multiple vulnerabilities. These vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, conduct URL spoofing, or bypass security restrictions. Details on obtaining the update release are available on Google's Chrome blog.
- Apple released Java for Mac OS X 10.5 Update 8 and Java for Mac OS X 10.6 Update 3 to address multiple vulnerabilities affecting the Java package. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code or cause a denial-of-service condition. Details on obtaining the updates can be found in Apple articles HT4417 and HT4418.
- Cisco released a security advisory cisco-sa-20101027-cs to address a vulnerability affecting CiscoWorks Common Services for Oracle Solaris and Microsoft Windows. This vulnerability may allow a remote, unauthenticated attacker to execute arbitrary code with administrative privileges or cause a denial-of-service condition.
- Mozilla released Firefox 3.6.12 and 3.5.15 to address an actively exploited vulnerability affecting the Firefox 3.5 and 3.6 web browser. This vulnerability may allow an attacker to execute arbitrary code. Additionally, this vulnerability has been addressed in Thunderbird 3.1.6 and 3.0.10.

Technical Cyber Security Alerts

Technical Cyber Security Alerts are distributed to provide timely information about current security issues, vulnerabilities, and exploits.

Technical Cyber Security Alerts for October 2010	
October 6	TA-10-279 Adobe Reader and Acrobat Affected by Multiple Vulnerabilities
October 12	TA-10-285 Microsoft Updates for Multiple Vulnerabilities
October 14	TA-10-287 Oracle Updates for Multiple Vulnerabilities

Cyber Security Alerts

Cyber Security Alerts are distributed to provide timely information about current security issues, vulnerabilities, and exploits. They outline the steps and actions that non-technical home and corporate users can take to protect themselves.

Cyber Security Alerts (non-technical) for October 2010	
October 6	Adobe Reader and Acrobat Affected by Multiple Vulnerabilities
October 12	Microsoft Updates for Multiple Vulnerabilities

Cyber Security Bulletins

Cyber Security Bulletins are issued weekly and provide a summary of new vulnerabilities recorded by the National Institute of Standards and Technology's (NIST's) National Vulnerability Database (NVD). The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / US-CERT. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

Security Bulletins for October 2010
SB10-277 Vulnerability Summary for the Week of September 27, 2010
SB10-284 Vulnerability Summary for the Week of October 4, 2010
SB10-291 Vulnerability Summary for the Week of October 11, 2010
SB10-298 Vulnerability Summary for the Week of October 18, 2010

A total of 297 vulnerabilities were recorded in the NVD during September 2010.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users. The September tip focused on end-user license agreements and file-sharing technology.

Cyber Security Tips for October 2010	
October 11	ST10-001 Recognizing Fake Antiviruses
September 29	ST05-017 Cybersecurity for Electronic Devices

Security Highlights

Recognizing Fake Antiviruses

What is fake antivirus?
Fake antivirus is malicious software (malware) designed to steal information from unsuspecting users by mimicking legitimate security software. The malware makes numerous system modifications making it extremely difficult to terminate unauthorized activities and remove the program. It also causes realistic, interactive security warnings to be displayed to the computer user.

How can my computer become infected with fake antivirus?
Criminals distribute this type of malware using search engines, emails, social networking sites, internet advertisements and other malware. They leverage advanced social engineering methodologies and popular technologies to maximize number of infected computers.

How will I know if I am infected?
The presence of pop-ups displaying unusual security warnings and asking for credit card or personal information is the most obvious method of identifying a fake antivirus infection.

What can I do to protect myself?

- Be cautious when visiting web links or opening attachments from unknown senders. See Using Caution with Email Attachments for more information.
- Keep software patched and updated. See Understanding Patches for more information on the importance of software patching.
- To purchase or renew software subscriptions, visit the vendor sites directly.
- Monitor your credit cards for unauthorized activity.

- To report Internet crime or fraud, contact the Internet Crime Complaint Center (http://www.ic3.gov).

Contacting US-CERT

If you would like to contact US-CERT to ask a question, submit an incident, or learn more about cyber security, please use one of the methods listed below. If you would like to provide feedback on this report, or if you have comments or suggestions for future reports, please e-mail info@us-cert.gov.

Web Site Address: http://www.us-cert.gov
E-mail Address: mailto:info@us-cert.gov
Phone Number: +1 (888) 282-0870
PGP Key ID: 0x91D70D64
PGP Key Fingerprint: EAAC 46A4 4CEC 8A78 EED2 73F3 E5F3 5D6C 91D7 0D64
PGP Key: https://www.us-cert.gov/pgp/info.asc